View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by CERN Document Server

3-Local Hamiltonian is QMA-complete

Julia Kempe * Oded Regev †

May 21, 2003

Abstract

It has been shown by Kitaev that the 5-LOCAL HAMILTONIAN problem is QMA-complete. Here we reduce the locality of the problem by showing that 3-LOCAL HAMILTONIAN is already QMA-complete.

1 Introduction

Complexity theory is one of the cornerstones of theoretical computer science, formalizing the notion of an *efficient* algorithm (see, e.g., [1]). With the advent of quantum computing a plethora of new complexity classes have entered the field. One of the major challenges for theoretical computer science is to understand their structure and the interrelation between classical and quantum classes.

A seminal result in classical complexity theory is the celebrated Cook-Levin theorem which states that SAT is NP-complete. Namely, we are given a set of clauses (disjunctions) over a set of n variables and asked whether there exists an assignment to the variables that satisfies all clauses. Moreover, the 3SAT problem in which each clause contains at most three literals is also NP-complete. It turns out that the 2SAT problem (where each clause contains at most two literals) can be solved in polynomial time (actually, there is even a linear time algorithm). However, the MAX2SAT problem in which we are given an extra number d and asked whether there exists an assignment that satisfies at least d clauses is still NP-complete.

In this paper we will be interested in the quantum analogues of the above results. For a good introduction the reader is referred to a recent survey by Aharonov and Naveh [2] and to a book by Kitaev, Shen and Vyalyi [3]. Kitaev defined a quantum analogue of the classical class NP and named it BQNP. Strictly speaking, this class is the quantum analogue of MA, the probabilistic version of NP, and hence we will call it QMA (as was done in [2]).

QMA is naturally defined as a class of promise problems: A promise problem L is a pair (L_{yes}, L_{no}) of disjoint sets of strings corresponding to "Yes" and "No" instances of the problem. The problem is to determine, given a string $x \in L_{yes} \cup L_{no}$, whether $x \in L_{yes}$ or $x \in L_{no}$. Let $\mathcal{B}$ be the Hilbert space of a qubit.

Definition 1.1 (QMA) *Fix $\varepsilon = \varepsilon(|x|)$ such that $2^{-\Omega(|x|)} \leq \varepsilon \leq \frac{1}{3}$. Then, a promise problem $L \in QMA$ if there exists a quantum polynomial time verifier V and a polynomial p such that:*

*CNRS-LRI UMR 8623, Université de Paris-Sud, 91405 Orsay, France and Computer Science Division and Department of Chemistry, UC Berkeley. E-Mail: kempe@lri.fr

†Institute for Advanced Study, Princeton, NJ. E-Mail: odedr@ias.edu.

- $\forall x \in L_{yes} \quad \exists |\xi\rangle \in \mathcal{B}^{\otimes p(|x|)} \quad Pr\left(V(|x\rangle, |\xi\rangle) = 1\right) \geq 1 - \varepsilon$

- $\forall x \in L_{no} \quad \forall |\xi\rangle \in \mathcal{B}^{\otimes p(|x|)} \quad Pr\left(V(|x\rangle, |\xi\rangle) = 1\right) \leq \varepsilon$

where $Pr\left(V(|x\rangle, |\xi\rangle) = 1\right)$ *denotes the probability that* V *outputs* 1 *given* $|x\rangle$ *and* $|\xi\rangle$.

By using amplification methods, it was shown in [3] that for any choice of ε in the above range the resulting classes are equivalent. In this paper we will assume that ε is $2^{-\Omega(|x|)}$.

We would also like to find an analogue of the SAT problem. One natural choice is the Local Hamiltonian problem. As we will see later, this problem is indeed a complete problem for QMA:

Definition 1.2 *We say that an operator* $H : \mathcal{B}^{\otimes n} \longrightarrow \mathcal{B}^{\otimes n}$ *on* n *qubits is a* k*-local Hamiltonian if* H *is expressible as* $H = \sum_{j=1}^{r} H_j$ *where each term is a Hermitian operator acting on at most* k *qubits.*

Definition 1.3 *The (promise) problem* k-local Hamiltonian *is defined as follows:*

- **Input:** *A* k*-local Hamiltonian on* n*-qubits* $H = \sum_{j=1}^{r} H_j$ *with* $r = poly(n)$. *Each* H_j *has a bounded operator norm* $\|H_j\| \leq poly(n)$ *and its entries are specified by* $poly(n)$ *bits. In addition, we are given two numbers* a *and* b *(with* $poly(n)$ *precision) such that* $b - a > 1/poly(n)$. *We are promised that the smallest eigenvalue of* H *is either at most* a *or larger than* b.

- **Output:**

  1 *if* H *has an eigenvalue not exceeding* a,

  0 *if all eigenvalues of* H *are larger than* b.

We note that the original definition required that $0 \leq H_j \leq 1$ (i.e., that both H_j and $I - H_j$ are nonnegative, meaning that they only have nonnegative eigenvalues). However, it is easy to see that the two definitions are equivalent: given H_j's such that $\|H_j\| \leq poly(n)$ for each j, normalize a, b and all the H_j's by a factor of $1/poly(n)$ such that $\|H_j\| \leq \frac{1}{2}$. Then, add half the identity to each H_j (such that $0 \leq H_j \leq 1$) and $\frac{r}{2}$ to a and b where r is the number of terms in H.

It can be seen that the k-local Hamiltonian problem is NP-hard for all $k \geq 2$. This was recently shown by Wocjan and Beth [4] (see also [2]). One possible proof is to show that for any $k \geq 2$ the problem is at least as hard as MAX-k-SAT. The idea is to represent the n variables by n qubits and represent each clause by a Hamiltonian. Each Hamiltonian acts on the k variables that appear in its clause. It 'penalizes' the assignment which violates the clause by increasing its eigenvalue. Therefore, the lowest eigenvalue of the sum of the Hamiltonians corresponds to the maximum number of clauses that can be satisfied simultaneously.

However, the only known QMA-completeness result was due to Kitaev which showed that the 5-local Hamiltonian problem is QMA-complete [3]. An interesting open question which was already mentioned in [2] is whether the locality 5 is optimal. Given that classically MAX2SAT is NP-complete we might hope to reduce the locality of the Hamiltonians. Our main theorem is the following:

Theorem 1.4 *The problem* 3-local Hamiltonian *is QMA-complete.*

We note that the 1-LOCAL HAMILTONIAN problem can be solved in polynomial time by a classical algorithm and is therefore unlikely to be QMA-complete. We leave the case of 2-LOCAL HAMILTONIAN as an open problem. Finally, we mention that using the methods of [5] one can show that the 2-LOCAL HAMILTONIAN problem is QMA-complete if we allow higher dimensional systems instead of qubits.

2 Kitaev's Construction

In this section we will recall Kitaev's proof that $O(\log n)$-LOCAL HAMILTONIAN is QMA-complete (his proof that 5-LOCAL HAMILTONIAN is QMA-complete follows by a simple modification and we will mention it later). The proof begins by showing that k-LOCAL HAMILTONIAN is indeed in QMA for any $k = O(\log n)$:

Lemma 2.1 ([3]) *The k-LOCAL HAMILTONIAN problem is in QMA for any $k = O(\log n)$.*

Then, it is enough to show that any problem L in QMA can be reduced to $O(\log n)$-LOCAL HAMILTONIAN. Let $U_x = V(|x\rangle, \cdot) = U_T \cdots U_1$ be a quantum circuit of size $T = poly(|x|)$ operating on $N = poly(|x|)$ qubits. Notice that the input $x \in L$ is encoded into the circuit. We assume without loss of generality that $T \geq N$ and that each gate U_i operates on two qubits. Moreover, we assume that initially, the first $m = p(|x|)$ qubits contain the proof and the remaining ancillary $N - m$ qubits are zero (see Definition 1.1). Finally, we assume that the output of the circuit is written in the first computation qubit (i.e., it is 1 if the circuit accepts). The Hamiltonian H that is constructed operates on a space of $n = N + \log(T + 1)$ qubits. The first N qubits represent the computation and the last $\log(T+1)$ qubits represent the possible values $0, \ldots, T$ for the clock. The Hamiltonian is constructed of three terms,

$$H = H_{in} + H_{out} + H_{prop}. \tag{1}$$

The terms are given by

$$\begin{aligned} H_{in} &= \sum_{i=m+1}^{N} |1\rangle_i\langle 1|_i \otimes |0\rangle\langle 0| \\ H_{out} &= |0\rangle_1\langle 0|_1 \otimes |T\rangle\langle T| \\ H_{prop} &= \sum_{t=1}^{T} H_{prop,t} \end{aligned} \tag{2}$$

and

$$H_{prop,t} = \frac{1}{2}(I \otimes |t\rangle\langle t| + I \otimes |t-1\rangle\langle t-1| - U_t \otimes |t\rangle\langle t-1| - U_t^\dagger \otimes |t-1\rangle\langle t|) \tag{3}$$

for $1 \leq t \leq T$ where $|\alpha\rangle_i\langle\alpha|_i$ is the projection on the subspace in which the i'th qubit is $|\alpha\rangle$. It is understood that the first part of each tensor product acts on the space of the N computation qubits and the second part acts on the clock qubits. U_t and $U_t^\dagger$ in $H_{prop,t}$ act on the same computational qubits as U_t does when it is employed in the verifier's circuit U_x. Intuitively, each Hamiltonian 'checks' a certain property by increasing the eigenvalue if the property doesn't hold: The Hamiltonian H_{in} checks that the input of the circuit is correct (i.e., none of the last $N - m$

computation qubits is 1), H_{out} checks that the output bit indicates acceptance and H_{prop} checks that the propagation is according to the circuit. Notice that these Hamiltonians are $O(\log n)$-local since there are $\log(T+1) = O(\log n)$ clock qubits. The proof is completed by the following lemmas and recalling that ε is chosen to be $2^{-\Omega(|x|)}$ so that $\frac{c}{T^3} - \frac{\varepsilon}{T+1} > 1/poly(n)$:

Lemma 2.2 ([3]) *Assume that the circuit U_x accepts with probability more than $1-\varepsilon$ on some input $|\xi, 0\rangle$. Then the Hamiltonian H has an eigenvalue smaller than $\frac{\varepsilon}{T+1}$.*

Lemma 2.3 ([3]) *Assume that the circuit U_x accepts with probability less than ε on all inputs $|\xi, 0\rangle$. Then all the eigenvalues of H are larger than $\frac{c}{T^3}$ for some constant c.*

Although the proof of this lemma will not be used in this paper, we sketch it here for completeness:

Proof sketch: We write $H = H' + H_{prop}$ where H' denotes $H_{in} + H_{out}$. We start by noticing that both H' and H_{prop} are non-negative Hamiltonians. We can lower bound the smallest non-zero eigenvalue of H' by 1 since it is the sum of commuting projections. It can also be shown that the smallest non-zero eigenvalue of H_{prop} is at least $\Omega(1/T^2)$. This, however, is not enough to prove the lemma since, for example, the null-spaces of H' and H_{prop} might have a non-trivial intersection (i.e., there exists a non-zero vector in their intersection).

The next step is to show that since the circuit U_x accepts with small probability, the angle between the null-spaces of H' and H_{prop} is not too small (in particular, this implies that the intersection of the two null-spaces is trivial). More specifically, we define the angle θ between the null-spaces of H' and H_{prop} by

$$\cos\theta = \max |\langle \eta_1 | \eta_2 \rangle|$$

where the maximum is taken over all η_1 in the null-space of H' and η_2 in the null-space of H_{prop}. Then, one can prove that $\sin^2\theta \geq \Omega(1/T)$. Finally, it can be shown that the smallest eigenvalue of $H = H' + H_{prop}$ can be lower bounded by the smallest eigenvalue among the non-zero eigenvalues of H' and H_{prop} times $2\sin^2\frac{\theta}{2}$. Hence, we get the lower bound

$$\Omega(1/T^2) \cdot 2\sin^2\frac{\theta}{2}$$

which is at least $\frac{c}{T^3}$ for some constant $c > 0$. ∎

3 The Construction

The result of the previous section can be improved to 5-LOCAL HAMILTONIAN by using a unary representation for the clock and noting that three clock qubits are enough to identify the current time step (and since two computation qubits are also required, we get 5-local Hamiltonians). In addition, one has to add a Hamiltonian that penalizes clock qubits which are 'illegal', i.e., that do not represent a legal unary encoding. For more detail, see [3]. In this section, we show how to use the result of the previous section to obtain the 3-LOCAL HAMILTONIAN result. Our construction follows the ideas of Kitaev's 5-local proof. The main difference is that our Hamiltonians use only one clock qubit instead of three. This requires another modification, namely, the penalty for illegal clock representations has to be considerably higher.

According to Lemma 2.1, 3-LOCAL HAMILTONIAN is in QMA. Hence, it is enough to show that any problem L in QMA can be reduced to the 3-LOCAL HAMILTONIAN problem. We are given a circuit $U_x = U_T \cdots U_1$ as in the previous section. We construct a Hamiltonian H that operates on a space of $N+T$ qubits. The first N qubits represent the computation and the last T qubits represent the clock. The Hamiltonian is constructed of four terms,

$$H = H_{in} + H_{out} + H_{prop} + H_{clock}. \tag{4}$$

The first three terms check that the input of the circuit is correct, that the output bit indicates acceptance and that the propagation is according to the circuit. As before, tensor products separate the computation qubits from the clock qubits:

$$\begin{aligned} H_{in} &= \sum_{i=m+1}^{N} |1\rangle_i\langle 1|_i \otimes |0\rangle_1\langle 0|_1 \\ H_{out} &= |0\rangle_1\langle 0|_1 \otimes |1\rangle_T\langle 1|_T \\ H_{prop} &= \sum_{t=1}^{T} H_{prop,t} \\ H_{prop,t} &= \frac{1}{2}(I \otimes |10\rangle_{t,t+1}\langle 10|_{t,t+1} + I \otimes |10\rangle_{t-1,t}\langle 10|_{t-1,t} - U_t \otimes |1\rangle_t\langle 0|_t - U_t^\dagger \otimes |0\rangle_t\langle 1|_t) \end{aligned} \tag{5}$$

for $2 \le t \le T-1$ and

$$\begin{aligned} H_{prop,1} &= \frac{1}{2}(I \otimes |10\rangle_{1,2}\langle 10|_{1,2} + I \otimes |0\rangle_1\langle 0|_1 - U_1 \otimes |1\rangle_1\langle 0|_1 - U_1^\dagger \otimes |0\rangle_1\langle 1|_1) \\ H_{prop,T} &= \frac{1}{2}(I \otimes |1\rangle_T\langle 1|_T + I \otimes |10\rangle_{T-1,T}\langle 10|_{T-1,T} - U_T \otimes |1\rangle_T\langle 0|_T - U_T^\dagger \otimes |0\rangle_T\langle 1|_T). \end{aligned}$$

For any $0 \le t \le T$, let $|\widehat{t}\rangle$ denote the state

$$|\underbrace{1\ldots1}_{t}\underbrace{0\ldots0}_{T-t}\rangle.$$

These are the legal unary representations. The last term is chosen to give a high penalty to states which do not contain a legal unary representation in the clock qubits:

$$H_{clock} = T^{12} \sum_{1 \le i < j \le T} |01\rangle_{ij}\langle 01|_{ij} \tag{6}$$

We denote the sum $H_{in} + H_{prop} + H_{out}$ of the computation related Hamiltonians by H_{comp}. Note that H is a sum of 3-local Hamiltonians of bounded norm which can be specified by a polynomial number of bits, as required by Definition 1.3. We note that some of the terms in H_{prop} are negative, but this is allowed by Definition 1.3.

Lemma 3.1 (Completeness) *Assume that the circuit U_x accepts with probability more than $1-\varepsilon$ on some input $|\xi, 0\rangle$. Then H has an eigenvalue smaller than $\frac{\varepsilon}{T+1}$.*

Proof: Consider the vector

$$|\eta\rangle \stackrel{def}{=} \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} U_t \cdots U_1 |\xi, 0\rangle \otimes |\widehat{t}\rangle. \tag{7}$$

Then,

$$\langle\eta|H|\eta\rangle = \langle\eta|H_{in}|\eta\rangle + \langle\eta|H_{prop}|\eta\rangle + \langle\eta|H_{clock}|\eta\rangle + \langle\eta|H_{out}|\eta\rangle \tag{8}$$

and it is easy to see that the first three terms are zero. Moreover, since U_x accepts with probability higher than $1-\varepsilon$,

$$\langle\eta|H_{out}|\eta\rangle < \frac{\varepsilon}{T+1}. \tag{9}$$

■

Lemma 3.2 (Soundness) *Assume that the circuit U_x accepts with probability less than ε on all inputs $|\xi,0\rangle$. Then all the eigenvalues of H are larger than $\frac{c}{T^3}$ for some constant c.*

Proof: Let $\mathcal{H}_{legal}$ denote the subspace spanned by states whose clock qubits represent a unary encoding. The orthogonal space is denoted by $\mathcal{H}_{illegal}$. We will use a simple upper bound on the operator norm of H_{comp} given by

$$||H_{comp}|| \leq ||H_{in}|| + ||H_{out}|| + \sum_{t=0}^{T} ||H_{prop,t}|| \leq N + 1 + 2T \leq 4T. \tag{10}$$

We will show that for any unit vector $|\eta\rangle$, $\langle\eta|H|\eta\rangle \geq \frac{c}{T^3}$. Write $|\eta\rangle = \alpha_1|\eta_1\rangle + \alpha_2|\eta_2\rangle$ with $|\eta_1\rangle \in \mathcal{H}_{legal}$, $|\eta_2\rangle \in \mathcal{H}_{illegal}$, $|||\eta_1\rangle|| = |||\eta_2\rangle|| = 1$ and $\alpha_1, \alpha_2 \in [0,1]$ with $\alpha_1^2 + \alpha_2^2 = 1$. If $\alpha_2 \geq \frac{1}{T^5}$ then

$$\langle\eta|H|\eta\rangle \geq \langle\eta|H_{clock}|\eta\rangle - ||H_{comp}|| \geq \alpha_2^2 \cdot T^{12} - 4T > 1. \tag{11}$$

It remains to consider the case $\alpha_2 < \frac{1}{T^5}$. Noting that $H_{clock} \geq 0$ we get:

$$\begin{aligned}
&\langle\eta|H|\eta\rangle = \langle\eta|H_{clock}|\eta\rangle + \langle\eta|H_{comp}|\eta\rangle \geq \langle\eta|H_{comp}|\eta\rangle = \\
&\alpha_1^2\langle\eta_1|H_{comp}|\eta_1\rangle + 2\alpha_1\alpha_2\mathrm{Re}(\langle\eta_1|H_{comp}|\eta_2\rangle) + \alpha_2^2\langle\eta_2|H_{comp}|\eta_2\rangle = \\
&\langle\eta_1|H_{comp}|\eta_1\rangle - \alpha_2^2\langle\eta_1|H_{comp}|\eta_1\rangle + 2\alpha_1\alpha_2\mathrm{Re}(\langle\eta_1|H_{comp}|\eta_2\rangle) + \alpha_2^2\langle\eta_2|H_{comp}|\eta_2\rangle \geq \\
&\langle\eta_1|H_{comp}|\eta_1\rangle - \frac{1}{T^{10}}||H_{comp}|| - \frac{2}{T^5}||H_{comp}|| - \frac{1}{T^{10}}||H_{comp}|| \geq \\
&\langle\eta_1|H_{comp}|\eta_1\rangle - \frac{8}{T^9} - \frac{8}{T^4} > \langle\eta_1|H_{comp}|\eta_1\rangle - \frac{9}{T^4},
\end{aligned} \tag{12}$$

where we used the bound on the operator norm $||H_{comp}||$. Therefore, it is enough to show that for any $\eta \in \mathcal{H}_{legal}$, $\langle\eta|H_{comp}|\eta\rangle \geq \frac{c}{T^3}$. We will show that by using Lemma 2.3:

$$\begin{aligned}
&\langle\eta|H_{comp}|\eta\rangle = \langle\eta|\Pi H_{comp}\Pi|\eta\rangle = \\
&\langle\eta|\Pi H_{in}\Pi|\eta\rangle + \langle\eta|\Pi H_{out}\Pi|\eta\rangle + \sum_{t=1}^{T}\langle\eta|\Pi H_{prop,t}\Pi|\eta\rangle
\end{aligned} \tag{13}$$

where Π is the projection on the subspace $\mathcal{H}_{legal}$. We compute $\Pi H_{comp}\Pi$:

$$\begin{aligned}
\Pi H_{in}\Pi &= \sum_{i=m+1}^{N} |1\rangle_i\langle 1|_i \otimes |\widehat{0}\rangle\langle\widehat{0}| \\
\Pi H_{out}\Pi &= |0\rangle_1\langle 0|_1 \otimes |\widehat{T}\rangle\langle\widehat{T}| \\
\Pi H_{prop,t}\Pi &= \frac{1}{2}(I \otimes |\widehat{t}\rangle\langle\widehat{t}| + I \otimes |\widehat{t-1}\rangle\langle\widehat{t-1}| - U_t \otimes |\widehat{t}\rangle\langle\widehat{t-1}| - U_t^\dagger \otimes |\widehat{t-1}\rangle\langle\widehat{t}|)
\end{aligned} \tag{14}$$

for $2 \leq t \leq T-1$ and

$$\begin{aligned} \Pi H_{prop,1}\Pi &= \frac{1}{2}(I \otimes |\widehat{1}\rangle\langle\widehat{1}| + I \otimes |\widehat{0}\rangle\langle\widehat{0}| - U_1 \otimes |\widehat{1}\rangle\langle\widehat{0}| - U_1^\dagger \otimes |\widehat{0}\rangle\langle\widehat{1}|) \\ \Pi H_{prop,T}\Pi &= \frac{1}{2}(I \otimes |\widehat{T}\rangle\langle\widehat{T}| + I \otimes |\widehat{T-1}\rangle\langle\widehat{T-1}| - U_T \otimes |\widehat{T}\rangle\langle\widehat{T-1}| - U_T^\dagger \otimes |\widehat{T-1}\rangle\langle\widehat{T}|). \end{aligned} \quad (15)$$

The Hamiltonian $\Pi H_{comp}\Pi$ acts on the Hilbert space $\mathcal{H}_{legal}$ whose dimension is $2^N \cdot (T+1)$. The Hamiltonian presented in Section 2 acts on a Hilbert space of the same dimension. In fact, notice that the two Hamiltonians are equivalent up to a renaming of the basis elements. Therefore, Lemma 2.3 implies that for any $\eta \in \mathcal{H}_{legal}$, $\langle\eta|H_{comp}|\eta\rangle \geq \frac{c}{T^3}$ which completes the proof. ■

Acknowledgments

We wish to thank Dorit Aharonov and Fréderic Magniez for useful discussions. JK's effort is sponsored by the Defense Advanced Research Projects Agency (DARPA) and Air Force Laboratory, Air Force Materiel Command, USAF, under agreement number F30602-01-2-0524. OR's research is supported by NSF grant CCR-9987845.

References

[1] C. Papadimitriou. *Computational Complexity*. Addison Wesley, Reading, Massachusetts, 1994.

[2] D. Aharonov and T. Naveh. Quantum NP - a survey. In *quant-ph/0210077, http://xxx.lanl.gov*, 2002.

[3] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and quantum computation*, volume 47 of *Graduate Studies in Mathematics*. AMS, 2002.

[4] P. Wocjan and T. Beth. The 2-local Hamiltonian problem encompasses NP. In *quant-ph/0301087, http://xxx.lanl.gov*, 2003.

[5] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Universality of adiabatic quantum computation with two-body interactions. In preparation.